INTERNATIONAL SEARCH REPORT

International Application No PCT/AU 89/00098

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [5]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int. Cl.[4] G06F 13/14, 13/38; H04L 9/00, 11/26

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC	G06F 13/14, 13/38; H04L 9/00, 11/26

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

AU : IPC as above

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
P,A	Patents Abstracts of Japan, E-699, page 165 JP,A, 63-212261 (BITSUGU SONS K.K.) 27 December 1988 (27.12.88)	
P,A	AU,A, 78322/87 (WANG LABORATORIES, INC.) 23 June 1988 (23.06.88)	
A	Patents Abstracts of Japan, P-667, page 67 JP,A, 62-197850 (MITSUBISHI ELECTRIC CORP.) 16 February 1988 (16.02.88)	
A	AU,A, 76214/87 (HONEYWELL BULL INC.) 4 February 1988 (04.02.88)	
A	AU,A, 76189/87 (AMERICAN TELEPHONE AND TELEGRAPH COMPANY) 4 February 1988 (04.02.88)	
A	EP,A2, 0223122 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 27 May 1987 (27.05.87)	
A	AU,A, 57948/86 (SIEMENS AKTIENGESELLSCHAFT) 4 December 1986 (04.12.86)	
A	AU,A, 24126/84 (559620) (TRW, INC.) 2 August 1984 (02.08.84)	

(continued)

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
8 June 1989 (08.06.89)	20 June 1989 (20.06.89)
International Searching Authority	**Signature of Authorized Officer**
Australian Patent Office	A.J. EVANS

Form PCT/ISA/210 (second sheet) (January 1985)

BNSDOCID: <WO__8908887A1_I_>

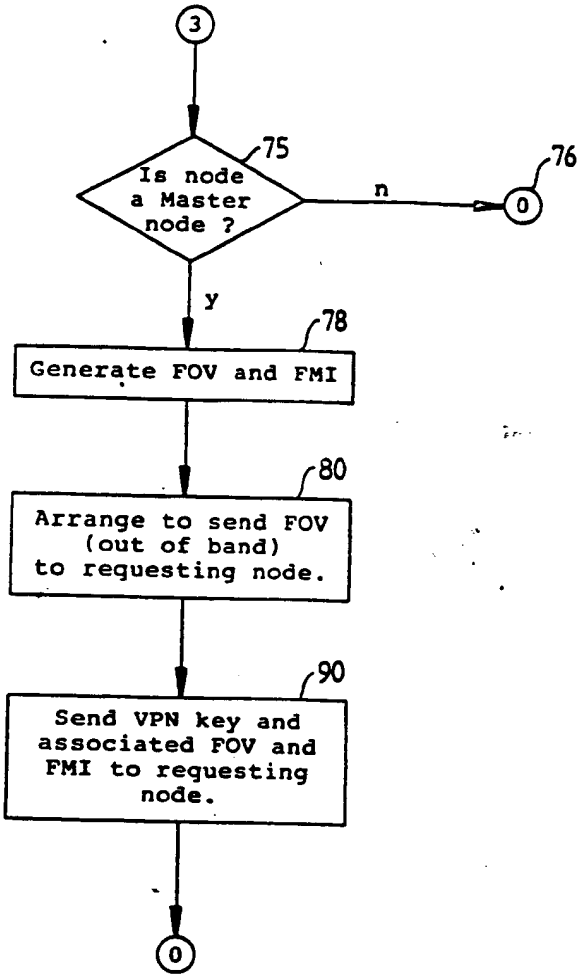


FIG 6C

BNSDOCID: <WO__8908887A1_I_>

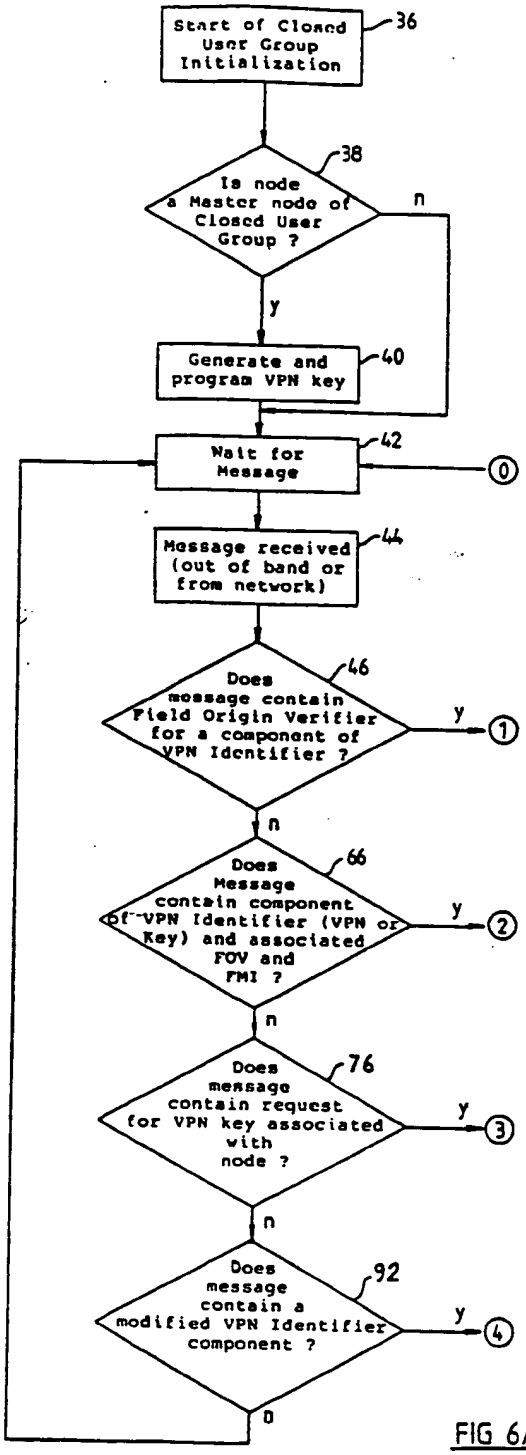
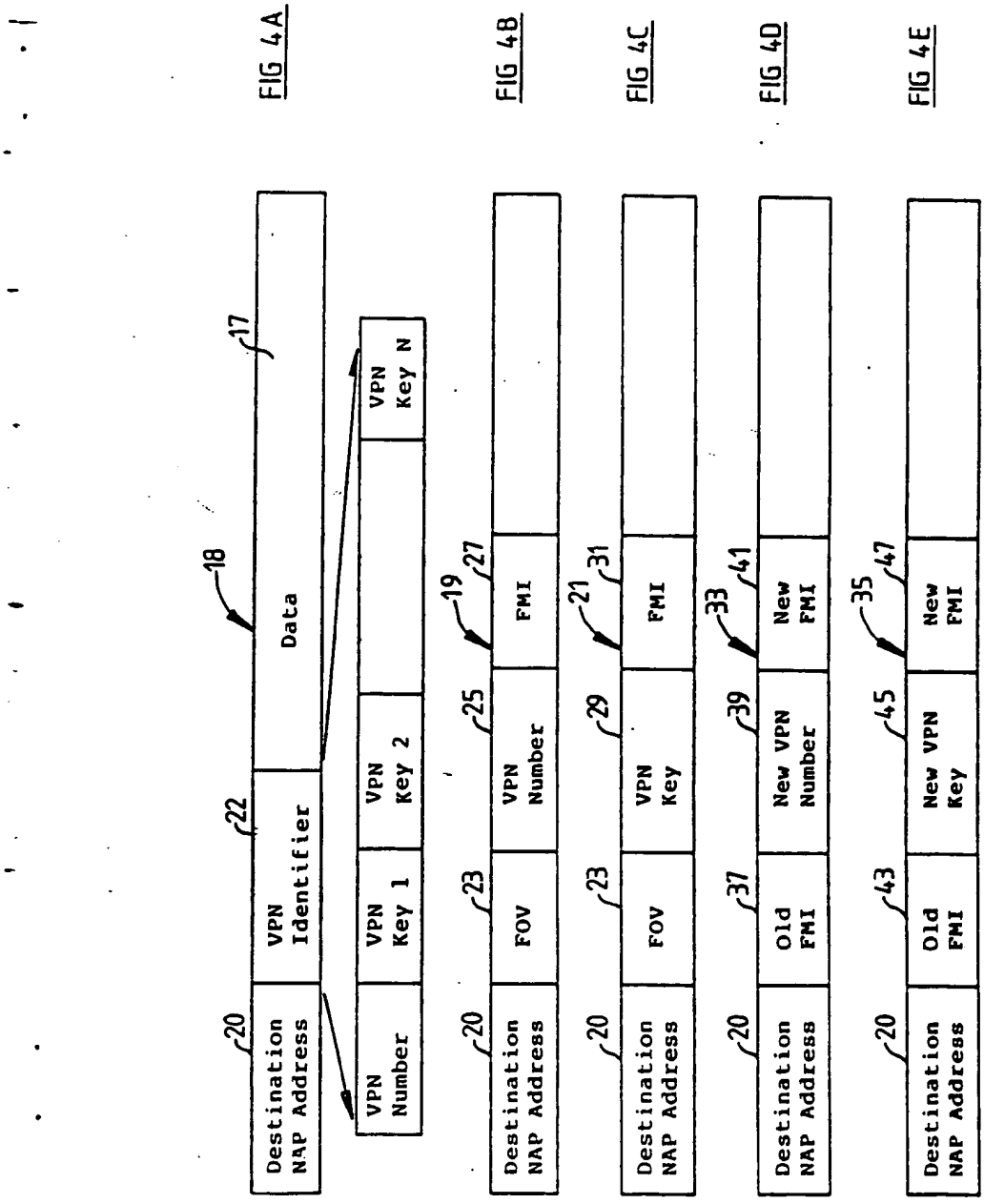


FIG 6A

BNSDOCID: <WO___8908887A1_I_>



SUBSTITUTE SHEET

BNSDOCID: <WO 8908887A1_I_>

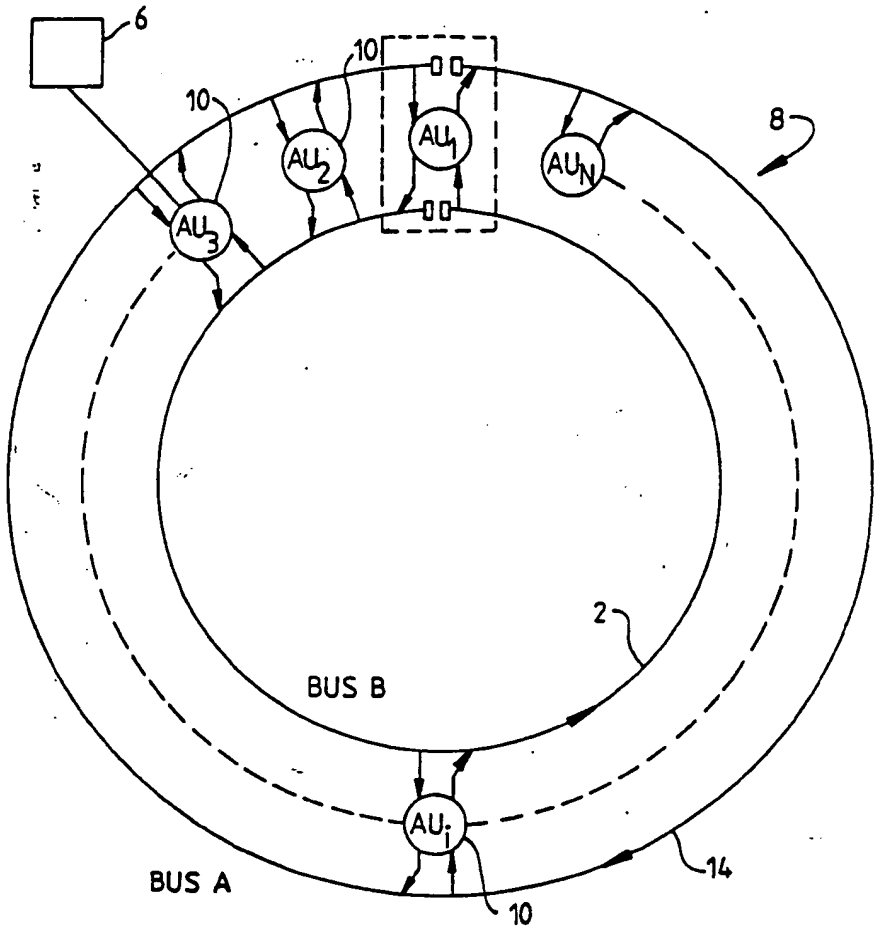


FIG 2

BNSDOCID: <WO__8908887A1_I_>

said packets which include FOVs also include Field Modification Indentifiers (FMI) fields and if there is correspondence between a third component of the security field stored at a node and the content of the FMI field, a change to the first and/or second component of the VPN Identifier field is permitted.

14. A method as claimed in claim 13 including the step of the transmitting from a master node or the network administrator to nodes in the closed user group a packet which includes a current FMI field, a new VPN Key field or VPN Number, respectively, and a new FMI field and permitting subsequent modifications of the VPN Identifier component only if there is correspondence between the third component and the content of the new field modification field.

15. A security system for a switched communications network (2), which includes a network administrator (6), and to which is attached a plurality of nodes (4), said system comprising means (10) for transmitting signals between said nodes in signal blocks (18) at least some of which include security fields (22), checking means at the nodes for checking the security fields to determine whether or not first and second components (VPN Number, VPN Key) thereof have particular characteristics, and wherein said network administrator includes means for generating the first component of the security field (VPN Number) and at least one of said nodes includes means for generating a second component (VPN Key) of the security field.

BNSDOCID: <WO__8908887A1_I_>

field (20), security field (22) and data field (17).

5. A method as claimed in claim 4 wherein the security access field includes a VPN Number field generated by the network administrator and a plurality VPN Key fields each associated with a master node in the group, the master nodes each being capable of providing VPN Keys, the other nodes not being capable.

6. A method as claimed in claim 5, wherein the method of establishing the closed user group includes the step of the master nodes of the closed user group requesting a VPN Number from the network administrator and themselves generating their respective fields of the VPN Key.

7. A method as claimed in claim 6 wherein a node requesting to join the closed user group, either during the initialization of the closed user group or to join an already existing closed user group, joins the closed user group through a multi-party rendezvous, wherein the network administrator supplies the requesting node with the VPN Number and the master nodes of the closed user group supply the requesting node with with the VPN Key fields, other than the VPN Key field which is supplied by the requesting node itself, in the case where the requesting node is also a master node of the closed user group.

8. A method as claimed in claim 7 including the step of transmitting from the network administrator to said requesting node a packet which includes a

BNSDOCID: <WO__8908887A1_I_>

security components from both the Network Administrator and the nodes. This makes the security system less vulnerable to unauthorised access, since the integrity of the system is not predicated upon the integrity of any single party.

Many modifications will be apparent to those skilled in the art.

ENSDOCID: <WO___8908887A1_I_>

been established. The VPN Identifier field 22 includes separate fields for the VPN Number and for VPN Key_1 to VPN Key_N, which is appropriate for a closed user group with N Master Nodes.

The packet formats 19 and 21 are appropriate when there is a request by a node to form or join a closed user group. The packet format 19 is typical of a packet which is sent by the Network Administrator 6 to a requesting node in order that the requesting node can complete its VPN Identifier. The packet 19 includes the destination NAP Address field 20, FOV field 23, which, as indicated previously, must be matched with the FOV conveyed to the requesting node out of band. It also includes a VPN Number field 25 which contains the VPN Number generated by the Network Administrator 6. Typically the VPN Number could comprise a randomly generated 16-bit number. The signal format also includes an FMI field 27 which is the password enabling subsequent authorized modification of the VPN Number in the field 25.

The packet format 21 shown in Figure 4B is appropriate for the signal sent by a Master Node when requesting to join or form a closed user group. The packet format 21 includes the address field 20, and an FOV field 23, which must match with that of the packet format of Figure 4B in order to establish or join the closed user group. The packet format includes a VPN Key field 29 which contains a coded number generated by the requesting node and which forms the other component of the VPN Identifier for the group. It also includes an FMI field 31 to

SUBSTITUTE SHEET (RULE 26)

step 72 thus holds up programming of the node until the FOV has been received from the out of band source.

Returning again to Figure 6A, if the step 66 yields a negative answer, the program passes to step 76. The step 76 enquires whether or not the message includes a request for a VPN Key. If yes, the program passes to step 75 shown in Figure 6C.

The step 75 determines whether or not the node is a Master Node. If it is not a Master Node, it cannot supply a VPN Key and therefore the program returns to Wait Step 42. If yes, the program generates an FOV and FMI, as indicated by step 78. The step 80 indicates the step of conveying the FOV out of band to the requesting node, for instance by secure courier. The program can then send the VPN Key and its associated FOV and FMI to the requesting node via the network, as indicted by step 90. The program then returns to Wait Step 42.

Returning once again to Figure 6A, if the step 76 yields a negative answer, program passes to step 92 which determines whether or not the message contains a modification for a component for the VPN Identifier and the associated FMI (indicated by a message type, for instance), which is transmitted when it is desired to change one or other VPN Identifier components. If the message is not of this type the program returns to Wait Step 42. If the received message does contain a modification to a VPN Identifier component the program passes to step 94 shown in Figure 6D.

BNSDOCID: <WO__8908887A1_I_>

FOV is discarded, as indicated by step 50 and the program returns to Wait Step 42. If the VPN Identifier component has not already been programmed, the program passes to step 52 which determines whether or not the corresponding component of the VPN Identifier i.e. the VPN Number or VPN Key, has already been received from messages from the network. If no, the program stores the FOV, as indicated by step 54 and then returns to a Wait Step 42. If the corresponding component has been received, the program passes to step 56.

In step 56, the program determines whether or not the FOV received from the Network is the same as that which has been received out of band. If the FOV received from the network is different, the program discards all stored fields i.e. any stored values for the VPN Number or VPN Key, as indicated by step 58 and then returns to Wait Step 42. If on the other hand the FOV's match, the program passes to step 60 which stores the received VPN Number from the Network Administrator or the received VPN Key from a Master Node. The program also stores a Field Modification Identifier (FMI) which a password associated with either the VPN Number or VPN Key. The FMI password enables authorized changes of the VPN Number or VPN Key to be made but only if there is a match of FMI's, as described hereinafter.
The program then passes to step 62 which determines whether all of the components of the VPN Identifier have been received. In the illustrated arrangement, when the VPN Key and VPN Number have both been received, the programming of the node is complete, as indicated by step 64 from which the program returns

BNSDOCID: <WO__8908887A1_I_>

Network Administrator. Users, via Master Nodes then program their own nodes with the associated VPN Keys. A particular VPN Key need not necessarily be known to any party other than the particular the user at a Master Node associated with that key.

The user at a node (either Master or Member) is then admitted in to the closed user group through a multi-party rendezvous at the Member's node, to program the node with the complete VPN Identifier. One example of the procedure for the multi-party rendezvous is described with reference to Figures 6A to D. The Network Administrator supplies the VPN Number and each Master Node supplies the corresponding VPN Key. The node being programmed permits the programming of the node with the appropriate fields (and supplies the appropriate Key if the node is also a Master Node). Typically, the communications with the node being programmed will occur over the network. Alternatively some communications with the node may be made by routes not including the network (out of band) for higher security.

In each case where a node must be programmed with either a VPN Number or Key, the particular field containing the VPN Number or Key may be associated with a "Field Origin Verifier" (FOV), which is a password distributed beforehand by the originator of the particular VPN Number or VPN Key to the node being programmed. Where the communication is out of band, the FOV can be conveyed to a node by secure courier or by other means. The data block carrying the particular VPN Number or Key will also carry the

BNSDOCID: <WO__8908887A1_I_>

message. The block 26 indicates that a message has been received from the network. The block 28 indicates extraction of the VPN Identifier from the message. In block 30, the VPN Identifier is checked to see whether it is the same as that which is stored in the node where the message is received. If yes, the nodes accepts the message, as indicated by block 32. If there is a mismatch, the node discards the message as indicated by block 34 and returns to the wait block 24. These logical steps are carried out by software in microcomputers at the nodes or in hard wired logic implemented to perform the same logical operations.

In accordance with the invention, the VPN Identifier is composed of two or more parts. The first part, referred to here as the "Virtual Private Network Number" (VPN Number), is allocated by the Network Administrator 6, which ensures that the VPN Number is both of a standard format and is unique within that subset of the communications network over which the security scheme extends. Because the Network Administrator 6 ensures that the VPN Number is unique, the entire VPN Identifier is hence unique. The remainder of the VPN Identifier, referred to herein as the "Virtual Private Network Key" (VPN Key), is provided by one or more of the nodes 4 in the closed user group defined by the particular VPN Identifier. These nodes are referred to as the "Master Nodes" of a particular closed user group (of which there may be one or more), as opposed to the "Member Nodes" of the closed user group (of which there may be zero or more). The nodes in the group agree that Master Nodes have the power to

INSDOCID: <WO 8908887A1 | >

FIGURES 4A to E show diagramatically typical signal formats;

FIGURE 5 is a block diagram showing essential steps of the technique of the invention; and

FIGURES 6A to D illustrate a more detailed flow chart of the steps of the invention.

Figure 1 is a schematic illustration of a switched communications network 2 having a plurality of nodes 4 attached thereto. The arrangement includes a Network Administration node 6. The Network Administrator node is generally responsible for administration of the network and performs such tasks as allocating addresses, charging, customer control etc. In the system of the invention, the Network Administrator is also partially involved in the initialization and administration of the security scheme, as will be described hereinafter.

Figure 2 shows a packet switched multi-access network 8 of the type disclosed in International Publication No. WO 86/03639, hereinafter referred to as a "QPSX" network. The QPSX network 8 can be considered as a more specific example of a network upon which the system of the invention can operate. The QPSX network 8 includes oppositely directed unidirectional buses 12 and 14 between which is connected a plurality of access units 10. Each of the access units 10 can be considered as a node in the schematic arrangement illustrated in Figure 1. The access units 10 provide access to users 16, as diagramatically illustrated in Figure 3. The user 16 uses the associated access unit 10 in order to receive and transmit data on the

BNSDOCID: <WO___8908887A1_I_>

is predicated upon the integrity of the Network Administrator. Examples of this technique are described in the following articles: M. St. Johns, "Draft Revised IP Security Option", RFC 1038, and L. Neitzel, "Proposal for an Optional Security LLC Sublayer", Proposal to IEEE 802.2.

The general object of the present invention is to overcome the drawbacks of the security techniques defined above.

According to the present invention there is provided a method of securely transmitting switched signals between nodes which are attached to a communications network, said communications network including a network administrator, said method including the steps of transmitting signals in blocks at least some of which include security fields, checking the security fields at the nodes and accepting the received signal at a node only if first and second components of the security field have a particular characteristic, and wherein the security field is established by generating the first component of the security field by the network administrator and generating the second component of the security field by at least one of the nodes.

The invention also provides a security system for a switched communications network which includes a network administrator and to which is attached a plurality of nodes, said system comprising means for transmitting signals between said nodes in signal blocks at least some of which include security fields, checking means at the nodes for checking the

BNSDOCID: <WO__8908887A1_I_>

One known practice for the operation of such networks described above is for a node to accept all blocks prefixed with a NAP Address associated with that node. There is no need for prior authorization from either the destination node or the Network Administrator, before a source node initiates a communication with a destination node. This approach has the drawbacks that a node is neither able to verify the identity or authorization of the source node before accepting the message, nor is the node able to regulate the nodes with which it is willing to communicate. Thus, there is little security in such a system.

One proposal for partially overcoming these problems is for a destination node to regulate the nodes with which it is authorized to engage in communication, on the basis of the NAP Addresses of the source nodes. A source node appends a NAP Address corresponding to that node to at least the first data block transmitted to the destination node. Then each destination node checks the NAP Address of the source node upon the initiation of a communication, against a list of the NAP Addresses of the nodes from which the node is authorized to receive data. The received data block is accepted only if the source node's NAP Address is found in the list of authorized nodes. The list of authorized nodes is programmed either by the destination node or by the Network Administrator. This approach has the drawback, however, that the security checking is performed upon the source node's NAP Address. Since this is appended by the source node, its integrity cannot be guaranteed. Furthermore, since the NAP

BNSDOCID: <WO__8908887A1_I_>

ACCESS SECURITY SYSTEM FOR SWITCHED COMMUNICATIONS NETWORKS

This invention relates to an access security system for switched communications networks.

The security system of the invention prevents unauthorized access to nodes attached or coupled to a switched communications network.

Normally it is not possible to access communications on the network other than through the nodes attached to the network. Typically a particular node is designated by one or more identifiers, Network Access Point Addresses (NAP Address), which uniquely identify the attachment point of that node throughout the network. An administrative entity is usually responsible for the allocation of NAP Addresses, and, for the purposes of this specification all entities responsible for the

BNSDOCID: <WO___8908887A1_I_>

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 4 : G06F 13/14, 13/38, H04L 9/00 H04L 11/26

A1

(11) International Publication Number: WO 89/ 08887

(43) International Publication Date: 21 September 1989 (21.09.89)

(21) International Application Number: PCT/AU89/00098

(22) International Filing Date: 10 March 1989 (10.03.89)

(31) Priority Application Number: PI 7205

(32) Priority Date: 11 March 1988 (11.03.88)

(33) Priority Country: AU

(71) Applicant *(for all designated States except US)*: QPSX COMMUNICATIONS LTD. [AU/AU]; 33 Richardson Street, West Perth, W.A. 6005 (AU).

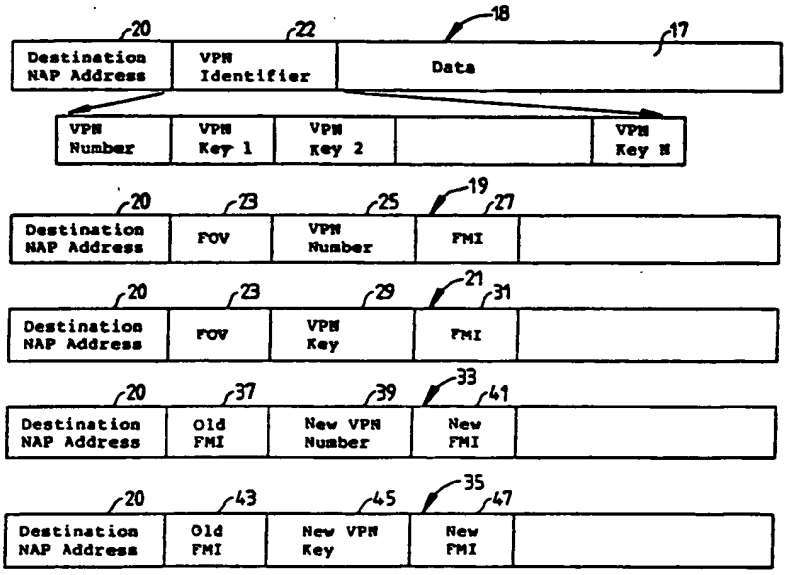
(72) Inventor; and
(75) Inventor/Applicant *(for US only)* : ALLES, Anthony, Lakshman [AU/AU]; Unit 10/152 Edinboro Street, Joondara, W.A. 6060 (AU).

(74) Agents: PRYOR, Geoffrey, C. et al.; Davies & Collison, 1 Little Collins Street, Melbourne, VIC 3000 (AU).

(81) Designated States: AT (European patent), AU, BE (European patent), CH (European patent), DE (European patent), FR (European patent), GB (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent), US.

Published
With international search report.

(54) Title: ACCESS SECURITY SYSTEM FOR SWITCHED COMMUNICATIONS NETWORKS



(57) Abstract

A method for securely transmitting signals in packets (18) between nodes (4) in a network (2), the method including the steps of providing in the packets security fields (22) which have first and second components, one of the components (VPN Number) being generated by the network administrator (6) and the second component (VPN Key) being generated by at least one of the nodes.

BNSDOCID: <WO__8908887A1_I_>